



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/567,584	10/30/2006	Masato Yamamichi	2006_0112A	2513
52349 7590 03/25/2009 WENDEROTH, LIND & PONACK L.L.P. 1030 15th Street, N.W. Suite 400 East Washington, DC 20005-1503				
EXAMINER VAUGHAN, MICHAEL R				
ART UNIT		PAPER NUMBER		
2431				
MAIL DATE		DELIVERY MODE		
03/25/2009		PAPER		

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

### Office Action Summary

**Application No.**

10/567,584

**Applicant(s)**

YAMAMICHI ET AL.

**Examiner**

MICHAEL R. VAUGHAN

**Art Unit**

2431

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 09 February 2009.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 22-37 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 22-37 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/CDC)
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date: \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_
- Paper No(s)/Mail Date: \_\_\_\_\_

### **DETAILED ACTION**

The instant application having Application No. 10/567584 is presented for examination by the examiner. Claims 1-21 have been canceled. Claims 22-37 have been added. Claims 22-37 have been examined.

### ***Response to Amendment***

#### ***Specification***

The disclosure has been amended and now overcomes the previous objection.

#### ***Claim Objections***

The previous claims have all been canceled and therefore the previous objections are moot.

#### ***Claim Rejections - 35 USC § 101***

The previous claims have all been canceled and therefore the previous rejections are moot.

### ***Response to Arguments***

Applicant's arguments with respect to claims 22-37 have been considered but are moot in view of the new ground(s) of rejection.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 22-27, and 34-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over USP Patent Application Publication 2003/0152222 to Nakano et al., hereinafter Nakano in view of Japanese Patent Application No. 2001-60286 to Katsumi.

As per claim 22, Nakano teaches a content reproduction system for use with a plurality of contents, the content reproduction system comprising: a recording medium (0044); a content distribution apparatus (0053); and a reproduction apparatus (0066), wherein the recording medium is operable to store a master key that is common to a plurality of contents and rule information that indicates a use rule that is common to the

plurality of contents,

wherein the content distribution apparatus includes:

a storage unit for storing a plurality of encrypted contents and a plurality of encrypted content keys associated with the plurality of encrypted contents, the plurality of encrypted contents being generated by encrypting each of the plurality of contents by using one or more of a plurality of content keys, the one or more of the plurality of content keys being uniquely assigned to the each of the plurality of contents, the plurality of encrypted content keys being generated by encrypting the plurality of content keys, respectively, using the master key (0118); and

a distribution unit operable to distribute an encrypted content and an encrypted content key associated with the encrypted content to the reproduction apparatus in response to a request from the reproduction apparatus (0119);

wherein the reproduction apparatus includes:

a reading unit operable to read out the master key and the rule information from the recording medium(0120);

an acquiring unit operable to request an encrypted content from the content distribution apparatus, and to acquire the requested encrypted content and an encrypted content key associated with the encrypted content (0149);

a decrypting unit operable to determine if the acquired encrypted content is permitted to be used, based on the use rule indicated by the rule information and, if the acquired encrypted content is permitted to be used, to acquire the content key by

decrypting the encrypted content key using the master key, and to generate a decrypted content using the acquired content key (0071 & 0120); and

a reproducing unit operable to reproduce the decrypted content, and wherein the recording medium is insertable into the reproduction apparatus and removable from the reproduction apparatus (0127).

Nakano teaches all of the limitations of this claim with the exception of not explicitly teaching that the encrypted content and encrypted content keys are not stored on the media. Nakano stores all of the keys and encrypted content on the media. Then the reproduction device uses its device key to unfold the layers of encrypted keys [starting with the master key] to ultimately reproduce the content. The separation of the encrypted content from the media/master key (key specific to a particular content) is not new in the art. In fact separation of keys and DRM from the content is known in the art. Katsumi teaches a system in which the decryption key and usage rights of the content are stored on the media but the encrypted content would be downloaded from a server to the reproduction device (0024). Obtaining the key from a separate channel would improve the security of the system. One of ordinary skill in the art could substitute known methods which yield predictable results. It is within the capabilities of one of ordinary skill in the art to separate the keys and usage information from the content in a way to further secure the system. Substituting this known method within the system Nakano renders the newly amended claim obvious. By separating the master key and usage information, the distribution unit does not need the recording medium. It simply would transit the encrypted content and content key to the reproduction apparatus

similar to how cable/satellite TV is broadcasted. The content still could not be reproduced without the separately obtained media which holds the encrypted master keys and usage information.

As per claim 23, Nakano teaches wherein the recording medium stores the master key as an encrypted master key generated by encrypting the master key using a device key uniquely assigned to the reproduction apparatus, and wherein the reading unit acquires the master key by decrypting the encrypted master key using the device key uniquely assigned to the reproduction apparatus (0119).

As per claim 24, 36, and 37, Nakano teaches a reproduction method, apparatus (playback device), and computer readable storage medium for use in a content reproduction system with a content distribution apparatus and a recording medium which stores a master key that is common to a plurality of contents and rule information that indicates a use rule that is common to the plurality of contents (0118),

wherein the content distribution apparatus is for storing a plurality of encrypted contents and a plurality of encrypted content keys associated with the plurality of encrypted contents, the plurality of encrypted contents being generated by encrypting each of the plurality of contents by using one or more of a plurality of content keys, the one or more of the plurality of content keys being uniquely assigned to the each of the plurality of contents, the plurality of encrypted content keys being generated by encrypting the plurality of content keys, respectively, using the master key (0018), and

wherein the content distribution apparatus is operable to distribute an encrypted content and an encrypted content key associated with the encrypted content to the

reproduction apparatus in response to a request from the reproduction apparatus (0119), the reproduction apparatus comprising:

- a reading unit operable to read out the master key and the rule information from the recording medium (0120);

- an acquiring unit operable to request an encrypted content from the content distribution apparatus, and to acquire the requested encrypted content and an encrypted content key associated with the encrypted content (0149);

- a decrypting unit operable to determine if the acquired encrypted content is permitted to be used based on the use rule indicated by the rule information, and if the acquired encrypted content is permitted to be used, operable to acquire the content key by decrypting the encrypted content key using the master key and to generate a decrypted content by decrypting the acquired encrypted content key using the acquired content key (0071 & 0120); and

- a reproducing unit operable to reproduce the decrypted content (0127).

Nakano teaches all of the limitations of this claim with the exception of not explicitly teaching that the encrypted content and encrypted content keys are not stored on the media. Nakano stores all of the keys and encrypted content on the media. Then the reproduction device uses its device key to unfold the layers of encrypted keys [starting with the master key] to ultimately reproduce the content. The separation of the encrypted content from the media/master key (key specific to a particular content) is not new in the art. In fact separation of keys and DRM from the content is known in the art. Katsumi teaches a system in which the decryption key and usage rights of the content

are stored on the media but the encrypted content would be downloaded from a server to the reproduction device (0024). Obtaining the key from a separate channel would improve the security of the system. One of ordinary skill in the art could substitute known methods which yield predictable results. It is within the capabilities of one of ordinary skill in the art to separate the keys and usage information from the content in a way to further secure the system. Substituting this known method within the system Nakano renders the newly amended claim obvious. By separating the master key and usage information, the distribution unit does not need the recording medium. It simply would transit the encrypted content and content key to the reproduction apparatus similar to how cable/satellite TV is broadcasted. The content still could not be reproduced without the separately obtained media which holds the encrypted master keys and usage information.

As per claim 25, Nakano teaches the recording medium stores the master key as an encrypted master key that is generated by encrypting the master key based on a device key uniquely assigned to the reproduction apparatus, and wherein the reading unit acquires the master key by decrypting the encrypted master key using a device key uniquely assigned to the reproduction apparatus (0119).

As per claim 26, Nakano teaches the recording medium stores another encrypted master key [unique media key] that is different from the encrypted master key, the another encrypted master key being generated by encrypting another master key (0131), the another master key being different from the master key, based on the device

key, and wherein the reading unit further acquires the another master key by decrypting the another encrypted master key using the device key (0140).

As per claim 27, Nakano teaches the recording medium stores the master key as an encrypted master key set [groups of unique media keys] that is generated by encrypting a master key set based on a device key uniquely assigned to the reproduction apparatus, the master key set including the master key and another master key that is different from the master key (0131), and wherein the reading unit acquires the master key set by decrypting the encrypted master key set using the device key uniquely assigned to the reproduction apparatus and acquires the master key from the acquired master key set (0131).

As per claim 32, Nakano is silent in disclosing the use rule indicates a value that has been prepaid as a payment for using the encrypted content, and wherein the decrypting unit is further operable to determine whether or not the encrypted content is permitted to be used in exchange for consuming the value indicated by the use rule, and operable to consume the value indicated by the use rule and decrypt the encrypted content if the encrypted content is permitted to be used in exchange for consuming the value indicated by the use rule. Katsumi teaches this limitation as a storing prepaid content information on a medium for the use of obtaining and decrypting content which is later downloaded (0008-0009). Examiner supplies the same rationale for the combination of Katsumi media into the system of Nakano as relied upon in the rejection of claim 22.

As per claim 34, Nakano teaches a content distribution apparatus for use in a content reproduction system with a reproduction apparatus and a removable recording medium which stores a master key that is common to a plurality of contents and rule information that indicates a use rule that is common to the plurality of contents (0119), the content distribution apparatus comprising:

a storage unit for storing a plurality of encrypted contents and a plurality of associated encrypted content keys associated with the plurality of encrypted contents, the plurality of encrypted contents being generated by encrypting each of the plurality of contents by using one or more of a plurality of content keys, the one or more of the plurality of content keys being uniquely assigned to the each of the plurality of contents, the plurality of encrypted content keys being generated by encrypting the plurality of content keys, respectively, using the master key (0118-0119); and

a distribution unit operable to distribute an encrypted content and an encrypted content key associated with the encrypted content to the reproduction apparatus in response to a request from the reproduction apparatus (0119).

Nakano teaches all of the limitations of this claim with the exception of not explicitly teaching that the encrypted content and encrypted content keys are not stored on the media. Nakano stores all of the keys and encrypted content on the media. Then the reproduction device uses its device key to unfold the layers of encrypted keys [starting with the master key] to ultimately reproduce the content. The separation of the encrypted content from the media/master key (key specific to a particular content) is not new in the art. In fact separation of keys and DRM from the content is known in the art.

Katsumi teaches a system in which the decryption key and usage rights of the content are stored on the media but the encrypted content would be downloaded from a server to the reproduction device (0024). Obtaining the key from a separate channel would improve the security of the system. One of ordinary skill in the art could substitute known methods which yield predictable results. It is within the capabilities of one of ordinary skill in the art to separate the keys and usage information from the content in a way to further secure the system. Substituting this known method within the system Nakano renders the newly amended claim obvious. By separating the master key and usage information, the distribution unit does not need the recording medium. It simply would transit the encrypted content and content key to the reproduction apparatus similar to how cable/satellite TV is broadcasted. The content still could not be reproduced without the separately obtained media which holds the encrypted master keys and usage information.

As per claim 35, Nakano teaches a master key storage unit for storing a plurality of master keys [inherent that is the content is encrypted with master keys, the original distributor must in fact possess those keys] and for storing a state for each master key of the plurality of master keys;

a state changing unit operable to set a state of a master key that is not permitted to be used among the plurality of master keys to an unusable state [media key information has some keys that have been revoke] (0136); and

a content key encrypting unit operable to generate an encrypted content key using a master key that is permitted to be used among the plurality of master keys (0136).

Claims 28-31 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nakano and Katsumi as applied to claim 24 above, and further in view of USP 6,240,401 to Oren et al., hereinafter Oren.

As per claim 28, Nakano teaches the recording medium contains use information [license number in the media number area] and a manipulating the media key so that the reproduction device can permit or deny (judge) whether or not the encrypted content can be reproduced (0140). Nakano also teaches an acquisition information storage sub-unit operable to store therein the received acquisition information in association with the encrypted content and the encrypted content key (0118). Nakano and Katsumi are silent in disclosing including use period information that indicates if the content is acquired for rent or purchase and judging based on those indicia whether or not to reproduce the content. Oren teaches including use period information that indicates if the content is acquired for rent or purchase and judging based on those indicia whether or not to reproduce the content (col. 6, lines 10-25). An obvious step of improvement would be to include this feature in the license information of Nakano system. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention

to modify the teachings of Nakano and Katsumi by including the use period information of Oren because it would allow the system to not only protect authorized copying but allow collection money base on the type of use. Nakano provides rationale for this where he teaches that reproduction only occurs if license information matches reference information (0222). Also pay-per-view is well known in the art. The acquiring unit of the claim would then receive the use period information stored from the purchased medium embodying the master keys and usage information. It is therefore inherent that the decryption unit would then take this information into consideration when determining whether or not to reproduce the content.

As per claim 29, Nakano and Katsumi are silent in disclosing if the acquisition information judging sub-unit judges that the acquisition information indicates rental, calculate a period between acquisition of the encrypted content and the encrypted content key and reception of the reproduction instruction, and judge whether the calculated period is within the use period indicated by the use period information. Oren teaches if the acquisition information judging sub-unit judges that the acquisition information indicates rental, calculate a period between acquisition of the encrypted content and the encrypted content key and reception of the reproduction instruction, and judge whether the calculated period is within the use period indicated by the use period information (col. 5, lines 55-61). Examiner incorporates the rationale for combining Nakano/Katsumi and Oren as applied to claim 7 above. It is obvious that if the media is rented to set some kind of time limit on the rental period, else, they user would get an unlimited playback having only paid for renting not owning.

As per claim 30, Nakano teaches the content-use recording medium further stores therein usable content information [media number and license information] that indicates a condition for using the content (0080), and the content information acquiring unit judges whether the condition for using the content is satisfied, acquires the encrypted content and the encrypted content key from the content distribution apparatus if having judged that the condition for using the content is satisfied, and does not acquire the encrypted content and the encrypted content key from the content distribution apparatus if having judged that the condition is not satisfied (0222).

As per claim 31, Nakano teaches the content distribution apparatus distributes the encrypted content and the encrypted content key to the reproduction apparatus regardless of whether the content distribution apparatus receives a content distribution request from the reproduction apparatus or not [broadcasted] (0059), and the acquiring unit is further operable to determine if the received encrypted content and encrypted content key satisfy the condition indicated by the usable content information, and operable to hold the received encrypted content and encrypted content key only if the received encrypted content and encrypted content key satisfy the condition indicated by the usable content information (0140-0141).

As per claim 33, Nakano and Katsumi are silent in explicitly teaching the use rule indicates a time period in which the encrypted content is permitted to be decrypted, and wherein the decrypting unit is further operable to determine if a current time is within the time period indicated by the use rule, and to decrypt the encrypted content if the current

time is within the time period. Oren teaches including use period information that indicates a time period in which the encrypted content is permitted to be decrypted and based on those indicia whether or not to reproduce the content (col. 6, lines 10-25). An obvious step of improvement would be to include this feature in the license information of Nakano system. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Nakano and Katsumi by including the use period information of Oren because it would allow the system to not only protect authorized copying but allow collection money base on the type of use. Nakano provides rationale for this where he teaches that reproduction only occurs if license information matches reference information (0222). It is therefore inherent that the decryption unit would then take this information into consideration when determining whether or not to reproduce the content.

***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/Ayaz R. Sheikh/

Supervisory Patent Examiner, Art Unit 2431